⑧(1)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-151578
(43)Date of publication of application : 30.05.2000

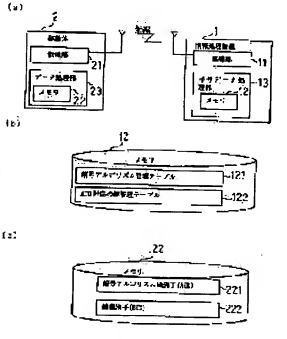
(51)Int.Cl. H04L 9/14
G07B 15/00
H04Q 7/38

(21)Application number : 10-318605
(22)Date of filing : 10.11.1998

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : MORIYOSHI KUNIHARU
TOKITA TOSHIO

(54) ENCRYPTION COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an encryption communication system where a mobile body and an information processing unit can process encryption communication by ensuring security of an encryption test possessed by the mobile body.
SOLUTION: A mobile body has plural encryption algorithm identifier AID 221 and a key identifier KID 222 of an encryption key/decoding key corresponding to the AID and an information processing unit has a plurality of encryption algorithm sets, the encryption algorithm identifier AID 221 corresponding to each encryption algorithm, a plurality of encryption keys/decoding keys corresponding to each encryption algorithm, the key identifier KID 222 corresponding to each encryption key/decoding key.



LEGAL STATUS

[Date of request for examination] 24.12.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

[0015]

[Means of solving the problems]

The encryption communication device according to the first invention consisting of an information processing unit and a plurality of mobile bodies to mutually communicate with the information processing device, wherein

each of the mobile bodies includes a means for receiving a cipher text transmitted from the information processing device, a first storing means to store a unique encryption algorithm identifier, a unique key identifier as well as the cipher text received, and a means for transmitting the encryption algorithm identifier, the key identifier and the cipher text stored in the first storing means to the information processing device, when its position from the information processing device attains a prescribed position,

the information processing device includes a means for receiving the cipher text, encryption algorithm identifier and the key identifier transmitted from mobile bodies located at the prescribed position, a second storing means to store a plurality of different algorithms each corresponding to the encryption algorithm identifiers held by each of the plurality of mobile bodies, and a plurality of different keys each corresponding to the key identifiers held by each of the plurality of mobile bodies, a selecting means including a means for selecting a key corresponding to the received encryption algorithm identifier from among the plurality of algorithms stored in the second storing means, and a means for selecting an algorithm corresponding to the received encryption algorithm identifier from among the plurality of algorithms stored in the second storing means, a decrypting means for decrypting the received cipher text with the key selected by the selecting means using the algorithm selected by the selecting means, an encrypting means for generating a new cipher text with processed information processed based on information decrypted by the decrypting means and with the key selected by the selecting means, using the algorithm selected by the selecting means, and a means for transmitting the cipher text generated by the encrypting means to the mobile bodies located at the prescribed position.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－151578 (P2000－151578A)
(43)公開日　平成12年５月30日(2000.5.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	３Ｅ０２７
Ｇ０７Ｂ　15/00		Ｇ０７Ｂ　15/00	Ｌ	５Ｊ１０４
	５１０		５１０	５Ｋ０６７
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	

審査請求　未請求　請求項の数５　ＯＬ　（全 16 頁）

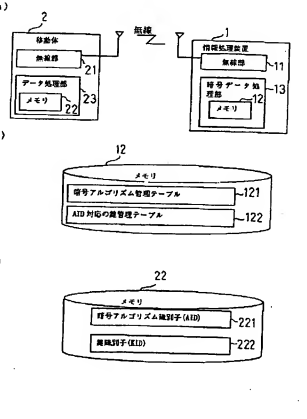
(21)出願番号　特願平10－318605
(22)出願日　平成10年11月10日(1998.11.10)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　森吉　国治
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　時田　俊雄
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外２名）

Ｆターム(参考)　3E027 EA01 EC07 EC10
5J104 AA34 DA03 NA40 PA01 PA11
5K067 AA30 AA34 AA35 EE02 HH36

(54)【発明の名称】　暗号通信装置

(57)【要約】
【課題】　従来の移動体と情報処理装置との間での暗号通信では、移動体において暗号化・復号化のための鍵、および暗号アルゴリズムを具備している。また、移動体、及び情報処理装置との間での通信において、使用される暗号化・復号化の鍵、および暗号アルゴリズムは各々固定されていたため、万一鍵情報が漏洩した場合は、暗号情報の盗聴やデータの改ざんの被害が拡大する危険があり、セキュリティの面から課題があった。また、移動体における暗号処理に絡むアプリケーションの種類は１種類に限定されていた。
【解決手段】　暗号アルゴリズム識別子（ＡＩＤ）と、ＡＩＤに対応した暗号鍵／復号鍵の鍵識別子（ＫＩＤ）複数個を移動体が具備し、複数の暗号アルゴリズムと、各々の暗号アルゴリズムに対応した暗号アルゴリズム識別子（ＡＩＤ）と、各々の暗号アルゴリズムに対応した複数の暗号鍵／復号鍵と、各々の暗号鍵／復号鍵に対応した鍵識別子（ＫＩＤ）とを情報処理装置が具備する。



【特許請求の範囲】

【請求項１】　情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の暗号アルゴリズム識別子と鍵識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項２】　情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の複数の異なる暗号アルゴリズム識別子と複数の異なる鍵識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に記憶された暗号アルゴリズム識別子と鍵識別子と上記第１の記憶手段に格納された暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択されたアルゴリズムで上記受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項３】　上記情報処理装置の上記選択手段は、上記受信した暗号鍵識別子または鍵識別子を変更する手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから上記受信した暗号アルゴリズム識別子あるいは上記変更された暗号アルゴリズム識別子のいずれか一方に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から上記受信した鍵識別子あるいは上記変更された鍵識別子のいずれか一方に対応する鍵とを選択する手段を備え、上記情報処理装置の送信手段は、上記暗号化手段で生成された暗号文とともに上記受信された暗号アルゴリズム識別子、及び鍵識別子を上記所定位置に有る移動体へ向けて送信する手段を備えたことを特徴とする請求項１もしくは２記載の暗号通信装置。

【請求項４】　情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、

上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の移動体識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された移動体識別子と暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、

上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、及び移動体識別子を受信する手段と、上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された移動体識別子に対応するアルゴリズムを選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された移動体識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記移動体からの暗号

文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したことを特徴とする暗号通信装置。

【請求項５】　上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたことを特徴とする請求項１から４記載の暗号通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、無線通信機能を有する移動体と情報処理装置との間での移動体通信システムにおいて通信情報を秘匿する暗号通信装置に関するものである。

【０００２】

【従来の技術】近年、携帯電話、自動車電話、テレターミナルシステム等の移動体通信システムにおいて、通信の秘匿のために暗号が利用される。一般的な移動体通信システムにおける暗号通信方式の運用の一例として特開平１－３０７３４１号公報に開示されるようなテレターミナルシステムを以下に示す。図８にそのテレターミナルシステムの構成例を示し、図８（ａ）はシステム構成を示し、図８（ｂ）は移動体のデータ処理部が有するメモリの構成を示し、図８（ｃ）は情報処理装置のデータ処理部が有するメモリの構成を示すものである。図８（ａ）において、無線部３１、及びデータ処理部３３を有する携帯端末のような移動体３と、無線部４１、及びデータ処理部４３を有する地上の情報処理装置（固定設備）４とが無線接続されており、この間のデータ通信においてはデータの盗聴・漏洩を防ぐために暗号通信処理が行われる。また、図８（ｂ）において移動体３のデータ処理部３３は、暗号アルゴリズム３２１、及び原始鍵３２２と原始鍵を元に新たに生成するＤＥＳ暗号鍵３２３が保持されるメモリ３２を具備している。また、図８（ｃ）において、情報処理装置４のデータ処理部４３は、暗号アルゴリズム４２１、原始鍵４２２、及び原始鍵を元に新たに生成されるＤＥＳ暗号鍵４２３が保持されるメモリ４２を具備している。図９は、テレターミナルシステムの暗号通信方式の例を示すフローチャートである。

【０００３】なお、図９において情報処理装置４の１台に対して、情報処理装置４と通信を行う移動体３は３ａ以外にも複数（移動体３ｂ・・・移動体３ｎ）存在する。

【０００４】図８、および図９に示した従来の暗号通信方式実施例の動作を以下に説明する。

【０００５】まず、移動体３ａ、および情報処理装置４の各々において、メモリ３２に記憶された原始鍵αまたはメモリ４２に記憶された原始鍵βによる公開鍵Ｘまたは公開鍵Ｙが生成され、この公開鍵を互いに送信することによって公開鍵を共有する（処理Ｓ１０１、処理Ｓ１０３）。つぎに、移動体３ａにおいては、原始鍵αと情報処理装置から受信した公開鍵ＹによるＤＥＳ暗号鍵Ｚの生成を行い（処理Ｓ１０４）、一方情報処理装置４では、原始鍵βと移動体３ａから受信した公開鍵ＸによるＤＥＳ暗号鍵Ｚの生成が行われる（処理Ｓ１０２）。なお、このとき移動体３ａと情報処理装置４は共通のＤＥＳ暗号鍵Ｚを所有し、それぞれメモリ３２およびメモリ４２に保持することになる。

【０００６】つぎに、移動体３ａにおいて、ＤＥＳ暗号鍵Ｚによる送信文の暗号化を行って暗号文を生成し（処理Ｓ１０５）、この暗号文を情報処理装置４へ送信する（処理Ｓ１０６）。

【０００７】つぎに、情報処理装置４において、移動体３ａからの暗号文が受信される（処理Ｓ１０７）。この暗号文がＤＥＳ暗号鍵Ｚで復号化され、平文が生成される（処理Ｓ１０８）。生成された平文に対して情報処理装置４において内部処理が行われ、この処理結果に基づき移動体への送信文が生成される。この生成された送信文（平文）が移動体３ａへ送信するためにＤＥＳ暗号鍵Ｚで暗号化されて暗号文が生成され、この暗号文が移動体３ａへ送信される（処理Ｓ１０９）。つぎに、移動体３ａにおいて情報処理装置４からの暗号文を受信し、ＤＥＳ暗号鍵Ｚによる暗号文の復号化が行われ、平文化することによって移動体での送信文の内部処理が行われる（処理Ｓ１１０）。

【０００８】以上の動作により、移動体３ａと情報処理装置４との間で暗号通信が行われる。

【０００９】また、移動体３ｂから３ｎと情報処理装置４との間においても、上記の手順と同様にして、暗号通信が行われる。

【００１０】一方、上記のテレターミナルシステム等のような移動体通信システムとは別に、近年、有料道路を利用する車両に搭載された車載機（移動体）と料金所との間で双方向通信を行い、その車載機から通行料を課金する料金収受システムのような移動体通信システムが提案されている。

【００１１】図１０は、この種の料金収受システムの使用形態の一例を示したものである。図において、車載機５を搭載した車両６が情報処理装置７に接続された料金所８の所定位置に接近すると、例えば料金所８に設けられた撮像機９が車両６のナンバープレートを読み取る、あるいは料金所７に設けられた無線アンテナ１０が移動

体から発信される固有の識別信号を受信することにより、車両６と情報処理装置７との間で互いに相手の正当性を認証する相互認証処理が行われる。相互認証処理で認証された車両６は、内部のメモリーに保持された契約情報（顧客番号、車両の種別等）と利用情報（有料道路の入口料金所の情報、利用時間等）を車載機５の無線アンテナ１０から送信する。情報処理装置７は、料金所８に設けられた無線アンテナ１０を介してこの車両６からの送信データを受信後、その受信された契約情報や利用情報に基づいて利用料金（通行料金）を計算し、無線アンテナ１０を介して車載機５にその利用料金を送信する。車載機５は、情報処理装置７からの利用料金を受信すると、内部のメモリーに記憶された所持金からこの利用料金を減算して所持金を更新し、内部のメモリーに格納する。

【００１２】この種の料金収受システムのような移動体通信システムにおいても、無線通信される利用情報や利用料金の盗聴、漏洩を防ぐために、データの秘匿が不可欠となる。このため、上述のテレターミナルシステム等の移動体通信システムと同様の図８，９に示すような暗号通信方式を利用したシステムが提案されている。

【００１３】

【発明が解決しようとする課題】従来の移動体と情報処理装置との間での暗号通信では、以上のように情報処理装置だけでなく、移動体においても暗号化・復号化のための鍵（暗号鍵、復号鍵）、および暗号アルゴリズムを具備している。また、移動体、および情報処理装置との間での通信において、使用される暗号化・復号化のための鍵（暗号鍵、復号鍵）、および暗号アルゴリズムは固定されていて、公開鍵と共通鍵で各々１種類である。このため、不特定多数の所有者が存在する移動体において、万一移動体での鍵管理が不徹底のために鍵情報が漏洩した場合は、鍵、および暗号アルゴリズムは１種類で固定されているので、暗号情報の盗聴やデータの改ざんの被害が拡大する危険があり、セキュリティの面から課題があった。また、移動体における暗号処理に絡むアプリケーションの種類は１種類に限定されていた。

【００１４】この発明は、上述のような課題を解決するためになされたもので、複数の暗号アルゴリズム、および当該暗号アルゴリズムに対応した複数の暗号鍵／復号鍵をシステムにて利用可能とすることにより、前記移動体が各々の暗号アルゴリズム処理、および当該暗号アルゴリズムに対応した暗号鍵／復号鍵の処理によるアプリケーション機能を実現し、かつ前記移動体が有する暗号文に対するセキュリティを確保して当該移動体と情報処理装置において暗号通信処理が可能な暗号通信装置を提供することを目的とするものである。

【００１５】

【課題を解決するための手段】第１の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の暗号アルゴリズム識別子と鍵識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に格納された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応する鍵を選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したものである。

【００１６】第２の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の複数の異なる暗号アルゴリズム識別子と複数の異なる鍵識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された暗号アルゴリズム識別子と鍵識別子と上記第１の記憶手段に格納された暗号文をともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、暗号アルゴリズム識別子、及び鍵識別子を受信する手段と、上記移動体が個々に有する暗号アルゴリズム識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する鍵識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された暗号アルゴリズム識別子に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から受信された暗号アルゴリズム識別子に対応する鍵を選択する手段を有する選択手段と、上記

選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記受信された暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された処理情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する送信手段とを具備したものである。

【００１７】第３の発明による暗号通信装置は、第１もしくは第２の発明において、上記情報処理装置の上記選択手段は、上記受信した暗号アルゴリズム識別子または鍵識別子を変更する手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから上記受信した暗号アルゴリズム識別子あるいは上記変更された暗号アルゴリズム識別子のいずれか一方に対応するアルゴリズムを選択する手段、及び上記記憶手段に記憶された複数の鍵から上記受信した鍵識別子あるいは上記変更された鍵識別子のいずれか一方に対応する鍵とを選択する手段を備え、上記情報処理装置の送信手段は、上記暗号化手段で生成された暗号文とともに上記受信された暗号アルゴリズム識別子、及び鍵識別子を上記所定位置に有る移動体へ向けて送信する手段を備えたものである。

【００１８】第４の発明による暗号通信装置は、情報処理装置と、この情報処理装置と双方向通信を行う複数の移動体とで構成される暗号通信装置において、上記移動体は、上記情報処理装置から送信される暗号文を受信する手段と、固有の移動体識別子とを格納するとともに、上記受信された暗号文を格納する第１の記憶手段と、上記情報処理装置との位置が所定位置に到達したときに、上記第１の記憶手段に格納された移動体識別子と暗号文とをともに上記情報処理装置へ向けて送信する手段とを具備し、上記情報処理装置は、上記所定位置に有る移動体から送信された暗号文、及び移動体識別子を受信する手段と、上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数のアルゴリズム、及び上記移動体が個々に有する移動体識別子にそれぞれ対応した異なる複数の鍵を格納する第２の記憶手段と、上記第２の記憶手段に記憶された複数のアルゴリズムから受信された移動体識別子に対応するアルゴリズムを選択する手段、及び上記第２の記憶手段に記憶された複数の鍵から受信された移動体識別子に対応する鍵を選択する手段を有する選択手段と、上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで上記移動体からの暗号文を復号化する復号化手段と、上記復号化手段で復号化された情報に基づいて処理された情報と上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する暗号化手段と、上記暗号化手段で生成された暗号文を上記所定位置に有る移動体へ向けて送信する手段とを具備したものである。

【００１９】第５の発明による暗号通信装置は、第１の発明から第４の発明において、上記暗号化手段は、上記復号化された情報に基づいて利用料金を計算し、上記復号化された情報の有する所持金とこの計算された利用料金との差から新たな所持金を計算し、この計算された所持金と当該情報処理装置に固有の情報とから上記選択手段で選択された鍵を用いて、上記選択手段で選択されたアルゴリズムで新たに暗号文を生成する手段を備えたものである。

【００２０】

【発明の実施の形態】実施の形態１．従来の移動体通信システムでは、移動体と情報処理装置の双方で同じ暗号アルゴリズム、および暗号化・復号化に用いる共通な鍵を備えて、通信情報を秘匿する暗号通信が行われていた。特に、図１０に示すような料金収受システムでは、移動体（車載機５）が料金所の所定位置に到達したとき、移動体と情報処理装置との間で相互認証処理が行われ、認証された移動体が料金所に設けられた情報処理装置へ向けて契約情報および利用情報を暗号化された暗号文として送信し、情報処理装置がその暗号文を復号化し、復号化された平文に基づいて移動体の利用料金が計算される。情報処理装置は、その計算結果を暗号化して移動体へ送信し、移動体の課金が行われる。このとき、従来の料金収受システムでは、移動体は暗号化された利用料金を受信後に、受信された利用料金を復号化し、内部メモリに格納された所持金から復号化された利用料金を差し引いた残金を新たな所持金として計算し、その計算結果を内部メモリに格納していた。しかし、このような移動体通信においては、移動体が契約情報および利用情報に加えて残金を情報処理装置に送信後、情報処理装置が、移動体から送信された契約情報および利用情報に基づいて利用料金を計算し、また移動体から送信された所持金からその利用料金を差し引いて新たな所持金を計算し、その計算結果を移動体に送信するような利用形態も想定される。この利用形態においては、移動体と情報処理装置間で通信される暗号文の暗号化や復号化を情報処理装置が行い、情報処理装置から送信される暗号文を移動体の内部メモリに格納することによって、移動体では暗号文の生成や復号化を行わず、すなわち移動体に暗号アルゴリズムを持たせずに通信情報を秘匿することができる。この発明の実施の形態１は、このような運用に基づいて行われるもので、通信される暗号文の暗号化および復号化を情報処理装置のみで行い、移動体は、暗号文とともにその暗号文を暗号化するための暗号アルゴリズムと鍵を識別する識別子を情報処理装置へ送信し、情報処理装置は、その識別子に対応する暗号アルゴリズムと鍵によって暗号化された暗号文を移動体へ送信する暗号通信装置を提供するものである。以下、この発明による暗号通信装置の実施の形態を図に基づいて説明する。

【００２１】図１は、実施の形態１を示す構成図で、図１（ａ）は移動体通信システムの構成、図１（ｂ）は図１（ａ）の情報処理装置１のメモリ１２、図１（ｃ）は図１（ａ）の移動体２のメモリ２２を示すものである。同図（ａ）において、１は図１０に示された料金所８に設けられた情報処理装置、２は図１０に示された車両６に設けられた車載機５のように情報処理装置１と通信を行う移動体、１１は情報処理装置１の無線部、２１は移動体２の無線部、１２は情報処理装置１の暗号データ処理部１３のメモリ、２２は移動体２のデータ処理部２３のメモリである。メモリ２２は移動体２が情報処理装置１と送受信を行うための暗号文を格納するために、またメモリ１２は情報処理装置１が移動体２と送受信を行うための暗号文を格納したり、暗号化・復号化の処理や内部処理（例えば料金計算処理等）を行うために使用する。尚、情報処理装置１の１台が処理対象とする移動体２は複数台存在する。同図（ｂ）は情報処理装置１のメモリ１２を示すもので、暗号文の格納領域の他に、暗号アルゴリズム管理テーブル１２１、および暗号アルゴリズム識別子（以下ＡＩＤと称する）対応の鍵管理テーブル１２２を具備している。同図（ｃ）は移動体２のメモリ２２を示すもので、暗号文や内部処理のための格納領域の他に、２２１および２２２の領域にＡＩＤ、および鍵識別子（以下ＫＩＤと称する）が格納されている。ＡＩＤ、ＫＩＤは情報処理装置側で管理する識別子であり、個々の識別子が区別できるものであれば、例えば文字列と数字の組み合わせ（ＡＩＤ１，ＡＩＤ２，・・・ＡＩＤｎ）（ＫＩＤ１，ＫＩＤ２，・・・ＫＩＤｎ）やビットアサイン（数）による識別でよい。

【００２２】図２は、図１（ｂ）における情報処理装置１がメモリ１２に保持する暗号アルゴリズム管理テーブル１２１の詳細図である。同図において、１２１はシステムで定めている暗号アルゴリズムの識別子ＡＩＤ（１）からＡＩＤ（Ｋ）までの管理テーブル、ＡＩＤ（１）からＡＩＤ（Ｋ）に対応する暗号アルゴリズム１２１１のインデックス（メモリアドレス）、およびＡＩＤ（Ｋ）対応の鍵管理テーブル１２２のインデックス（メモリアドレス）を含む。

【００２３】図３は、図１における情報処理装置が保持するＡＩＤ（Ｋ）対応の鍵管理テーブル１２２であり、暗号鍵／復号鍵の鍵識別子ＫＩＤ、およびＫＩＤ対応の鍵（暗号鍵／復号鍵）を示すもので、一つのＡＩＤに対して、ＫＩＤとＫＩＤ対応の鍵がｎ個設定される。同図において、１２２１は一つのＡＩＤに対するｎ番目の鍵識別子ＫＩＤ（ｎ）であり、１２２２はＫＩＤ（ｎ）対応の鍵を指す。

【００２４】次に動作について説明する。本発明では、移動体では暗号アルゴリズムを具備しておらず、データが暗号化された状態のままで保存されることが前提となる。図４は、実施の形態１の処理手順を示すフローチャートである。図４における処理手順について述べる。まず、移動体２が情報処理装置７の設けられた料金所の所定位置に接近すると、相互認証の結果認証された移動体２にて情報処理装置１へ送信する暗号文とその暗号文に対応するＡＩＤ、ＫＩＤを移動体のメモリ２２から得る（処理Ｓ１）。この時、例えば暗号文として契約情報（顧客番号、移動体の種別等）や利用情報（有料道路の場合は前回通過した料金所にて送信された入口料金所の情報を示す入口情報、有料設備の場合は利用開始時間等）と移動体２の電子的に有する貨幣と等価な所持金の情報を得る。つぎに、このＡＩＤ、ＫＩＤ、および暗号文を情報処理装置１へ送信する（処理Ｓ２）。情報処理装置１では移動体２からＡＩＤ、ＫＩＤ、および暗号文を受信後（処理Ｓ３）、メモリ１２のアルゴリズム管理テーブル１２１より該当ＡＩＤの暗号アルゴリズムを選択する（処理Ｓ４）、ＡＩＤ対応の鍵管理テーブル、およびＫＩＤより暗号鍵／復号鍵を選択する（処理Ｓ５）。つぎに、選択された復号鍵をキーにして移動体２からの暗号文を選択された暗号アルゴリズムで復号して内部処理を行う（処理Ｓ６）。内部処理として、例えば、有料道路・有料設備の利用料金計算処理等を行う。有料道路利用の出口料金所の場合は、移動体２より受け取った顧客番号、移動体の種別（車両の種別）、入口情報と情報処理装置１の所在する出口料金所の情報に基づいて、情報処理装置が移動体２から受け取った所持金から利用料金（通行料金）を差し引いた残金を、新たな所持金として計算し、入口情報を初期値にする。また、入口料金所の場合は、入口情報のみ更新し、入口料金所の識別情報を付加する。この内部処理の結果得られる所持金と入口情報と契約情報から、暗号鍵をキーにして移動体への送信暗号文（応答暗号文）を生成し、移動体２へ送信する（処理Ｓ７）。移動体２では、情報処理装置１からの応答暗号文を受信（処理Ｓ８）して、受信暗号文のメモリ２２への格納等の内部処理を行う（処理Ｓ９）。この結果、移動体２では、新たな所持金を暗号化された状態でメモリ２２へ格納することになる。

【００２５】以上のように、この実施の形態１の複数暗号処理方式によれば、ＡＩＤとＡＩＤに対応したＫＩＤを移動体２が具備することで、移動体２では暗号化・復号化を行わず、情報処理装置１に暗号化・復号化の処理を任せることができる。尚、ＡＩＤ、ＫＩＤ、契約情報、利用情報、および所持金は移動体がシステム加入時（契約時）、システムによって移動体２に固定情報として組み込まれる。また、この所持金は、プリペードカードのように貨幣に等しいもの以外の、例えば、クレジットカードのように電子決裁されて移動体利用者の銀行口座から引き落とされるものでもよい。この場合、情報処理装置２が所持金の情報を銀行との間で送受信する。また、本方式では移動体２の内部には暗号アルゴリズムや暗号鍵・復号鍵を保有していないので、情報処理装置１

のＡＩＤ対応の鍵管理テーブル情報を盗まれない限り、移動体２の暗号化情報に対するセキュリティ確保に貢献できる。尚、上述の例は移動体（車両）が有料道路・設備を利用する料金収受システムについて示したが、移動体としては無線部、ＣＰＵ、メモリを有するＩＣカードであっても本発明は適用できる。また、移動体２のメモリ２２に記憶される暗号文は、所持金の代わりに利用料金であってもよい。この場合、情報処理装置１は、移動体２の利用者の銀行口座から、この利用料金を差し引くような電子決裁を行う。

【００２６】実施の形態２．図５は、実施の形態２を示す構成図で、図５（ａ）は移動体通信システムの構成、図５（ｂ）は図５（ａ）の移動体２のメモリ２２、図５（ｃ）は図５（ｂ）のＡＩＤ・ＫＩＤ対応テーブル２２３を示すものである。図５において、１は情報処理装置、２は移動体、２２３は移動体２のメモリ２２が具備するＡＩＤ・ＫＩＤ対応テーブルである。

【００２７】次に動作について説明する。移動体２は、ＡＩＤ・ＫＩＤ対応テーブル２２３を具備しており、このＡＩＤ・ＫＩＤ対応テーブル２２３により、システムで決められた複数の暗号アルゴリズムに対応する暗号アルゴリズム識別子（ＡＩＤ）、および各々の暗号アルゴリズムに対応する複数の暗号鍵／復号鍵の鍵識別子（ＫＩＤ）を保持することになる。この仕組みにより、移動体２と情報処理装置１とにおいて、複数の暗号アルゴリズム、および各々の暗号アルゴリズムに対応する複数の暗号鍵／復号鍵による暗号情報の送信・受信を行えるようになる。

【００２８】以上のように、移動体２が具備するＡＩＤとＫＩＤの組み合わせが複数ある場合でも、移動体２が格納している各々の暗号化情報に対応するＡＩＤ、ＫＩＤを暗号化情報とともに情報処理装置１に送信することで、情報処理装置１に暗号化・復号化の処理を任せることができる。

【００２９】実施の形態３．図６は、実施の形態３による複数暗号処理方式を示す構成図である。同図において、情報処理装置１は、暗号アルゴリズム管理テーブル、およびＡＩＤ対応の鍵管理テーブルを具備している。移動体２は、ＡＩＤ・ＫＩＤ対応テーブル２２３を具備し、ＡＩＤ・ＫＩＤ対応テーブル２２３には各ＡＩＤに対応したＫＩＤテーブルが含まれる。

【００３０】次に動作について説明する。移動体２が保持している暗号データと、その暗号データに関連するＡＩＤ、およびＡＩＤ・ＫＩＤ対応テーブル２２３中のＫＩＤテーブルから選択されたＫＩＤが、情報処理装置１へ送信される。情報処理装置１において、移動体２より受信したＡＩＤ、ＫＩＤを基にして、暗号アルゴリズム管理テーブル、ＡＩＤ対応の鍵管理テーブルから該当する暗号アルゴリズムと鍵を検出する。次に、この鍵で移動体２より受信した暗号データの復号化を行い、平文を得て内部処理を行い、移動体２への送信文（平文）を生成する。ここで、情報処理装置１において、移動体２への送信文（平文）を暗号化する際、暗号アルゴリズムや鍵を変更（更新、あるいは新規に設定）することができる。暗号アルゴリズムや鍵を変更した場合、ＡＩＤ、ＫＩＤも変更され、暗号化データとともに、移動体２へ送信される。移動体２では受信したＡＩＤ、ＫＩＤを基に、ＡＩＤ・ＫＩＤ対応テーブル２２３，２２３のＫＩＤテーブルの内容について、ＫＩＤの更新日を含めて更新処理を行う。

【００３１】以上のように、移動体２が保持する暗号データに関するＡＩＤとＫＩＤを変更する方式を提供することができる。

【００３２】実施の形態４．図７は、実施の形態４による複数暗号処理方式を示す構成図である。同図において、移動体２は移動体識別子（ＭＩＤ）２２４を具備している。情報処理装置１は、移動体識別子（ＭＩＤ）、および各ＭＩＤとＡＩＤ、ＫＩＤとの対応を判別できるＭＩＤ管理テーブル１２３を具備している。また、情報処理装置１は、ＭＩＤ管理テーブル１２３とリンクした暗号アルゴリズム管理テーブル１２１、暗号アルゴリズム管理テーブルとリンクしたＡＩＤ対応の鍵管理テーブル１２２を具備している。ＡＩＤ対応の鍵管理テーブル１２２の構成は図３と同様である。実施の形態４による複数暗号処理方式によれば、移動体２は移動体識別子（ＭＩＤ）２２４を具備していて、このＭＩＤのみを情報処理装置１へ送信することで、情報処理装置１において、ＭＩＤ管理テーブル１２３にて暗号アルゴリズム管理テーブル１２１、およびＡＩＤ対応の鍵管理テーブル１２２がリンクされることになり、移動体２と情報処理装置１との間での複数暗号処理を可能とする。

【００３３】

【発明の効果】この発明は、以上のように構成されるため、以下に示す効果を奏する。

【００３４】第１、および第５の発明によれば、移動体が当該システムで決められた暗号アルゴリズムや暗号鍵／復号鍵を具備していなくても、その対応する暗号アルゴリズム識別子や鍵識別子を具備することによって、これらの移動体と情報処理装置において、復号処理が可能な方式を提供することができる。これによって、移動体が有する暗号文に対する高セキュリティを確保することができる。

【００３５】また、第２の発明によれば、複数の暗号アルゴリズム、および当該暗号アルゴリズムに対応した複数の暗号鍵／復号鍵をシステムにて利用可能とすることにより、前記移動体が各々のアプリケーション処理に応じた暗号アルゴリズム処理、および当該暗号アルゴリズムに対応した暗号鍵／復号鍵を選択することが可能となり、各々の移動体のアプリケーションのセキュリティレベルに応じた暗号を選択することができる。

【００３６】また、第３の発明によれば、移動体が具備する暗号アルゴリズム識別子と鍵識別子の変更を可能とする方式を提供することができ、暗号アルゴリズムや暗号鍵の変更に対して、柔軟に対応することができる。

【００３７】また、第４の発明によれば、移動体が具備する移動体識別子を情報処理装置が認識することで、移動体がシステムで決められた複数の暗号アルゴリズムの何れで処理しても、かつ、移動体がシステムで決められた複数の暗号鍵／復号鍵の何れで処理しても、移動体と情報処理装置において暗号処理が可能な方式を提供することができる。

【図面の簡単な説明】

【図１】　この発明の実施の形態１を示す構成図である。

【図２】　この発明の実施の形態１を示す詳細構成図である。

【図３】　この発明の実施の形態１を示す詳細構成図である。

【図４】　この発明の実施の形態１の処理手順を示すフローチャートである。

【図５】　この発明の実施の形態２を示す構成図である。

【図６】　この発明の実施の形態３を示す構成図である。

【図７】　この発明の実施の形態４を示す構成図である。

【図８】　従来の移動体通信における暗号処理方式の構成図である。

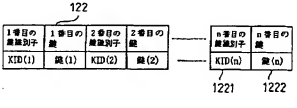
【図９】　従来の移動体通信における暗号処理方式の処理手順を示すフローチャートである。

【図１０】　料金収受システムの構成例である。

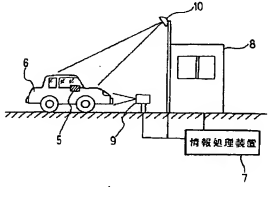
【符号の説明】

１　情報処理装置、２　移動体、３　移動体、３ａ　移動体、３ｂ　移動体、４　情報処理装置、５ａ　移動体、５ｂ　移動体、５ｎ　移動体、６　情報処理装置、１１　無線部、１２　メモリ、２１　無線部、２２　メモリ、３１　無線部、３２　メモリ、４１　無線部、４２　メモリ、５１　無線部、５２　メモリ、５３　データ処理部、６１　無線部、６２　メモリ、６３　データ処理部、１２１　暗号アルゴリズム管理テーブル、１２２　ＡＩＤ対応の鍵管理テーブル、１２３　移動体識別子（ＭＩＤ）管理テーブル、２２１　暗号アルゴリズム識別子（ＡＩＤ）、２２２　鍵識別子（ＫＩＤ）、２２３　ＡＩＤ・ＫＩＤ対応テーブル、２２４　移動体識別子（ＭＩＤ）、３２１　暗号アルゴリズム、３２２原始鍵、３２３　新しい鍵、４２１　暗号アルゴリズム、４２２　原始鍵、４２３　新しい鍵、５２１　暗号管理情報、５２２　暗号文、６２１　暗号管理情報、６２２　暗号文、６２３　平文、１２１１　ＡＩＤ（Ｋ）の暗号アルゴリズム、１２２１　ＫＩＤ（ｎ）、１２２２　鍵。

【図３】

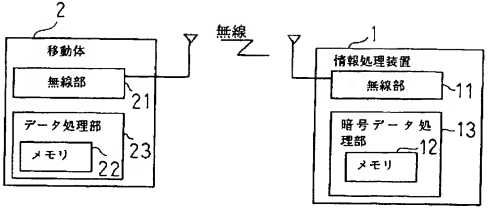


【図１０】

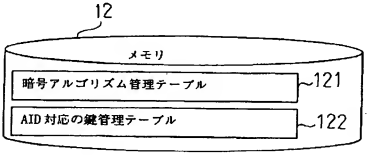


【図1】

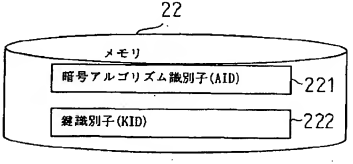
(a)



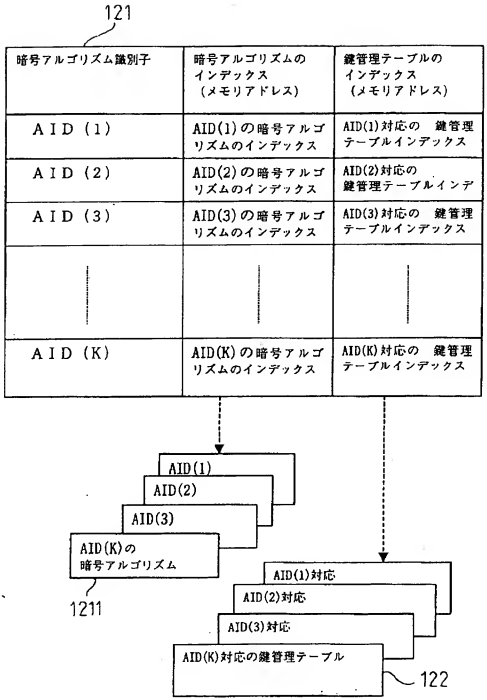
(b)



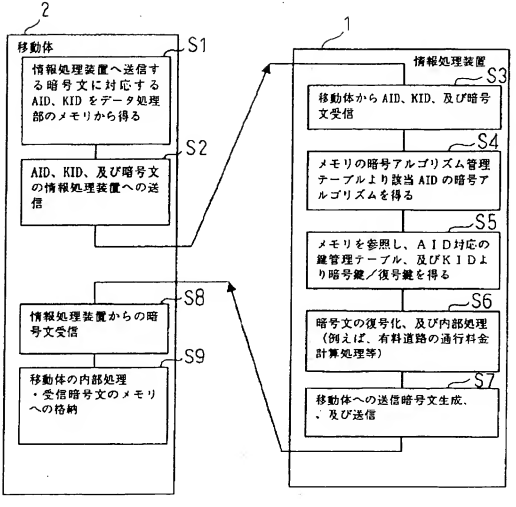
(c)



【図2】

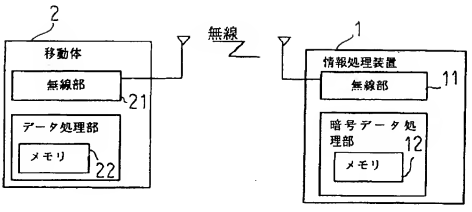


【図4】

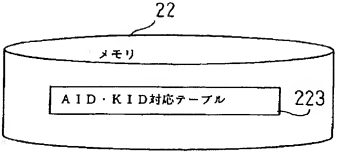


【図5】

(a)



(b)

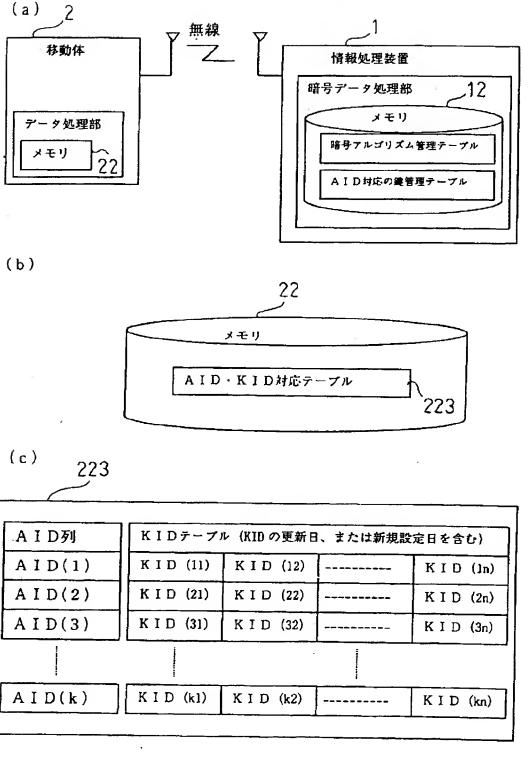


(c)

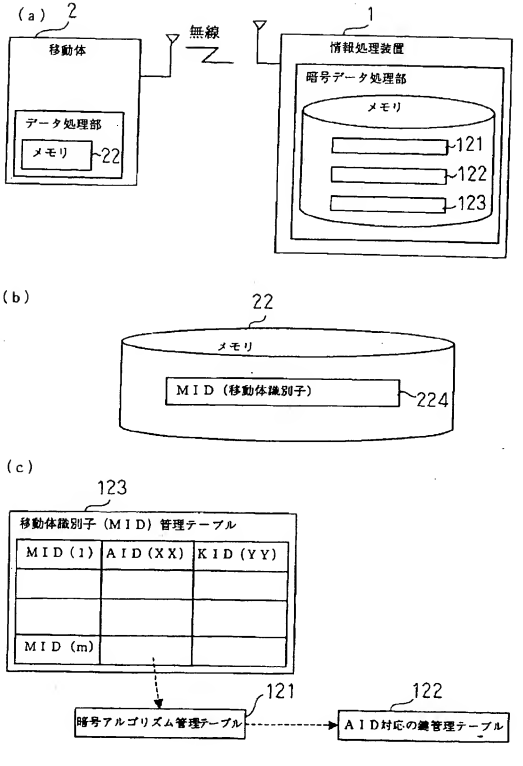
223

AID列	KIDテーブル			
AID(1)	KID (11)	KID (12)	----------	KID (1n)
AID(2)	KID (21)	KID (22)	----------	KID (2n)
AID(3)	KID (31)	KID (32)	----------	KID (3n)
AID(k)	KID (k1)	KID (k2)	----------	KID (kn)

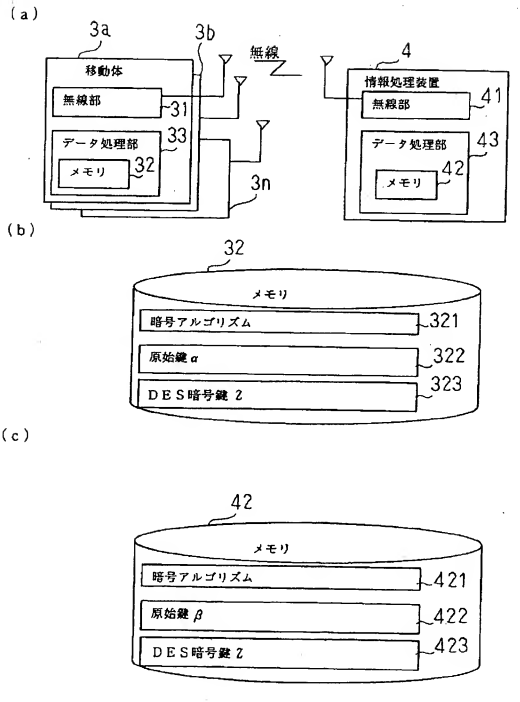
【図６】



【図７】



【図８】



【図9】